Europ. J. Combinatorics (1996) **17,** 309–316

Consequences of the Brylawski–Lucas Theorem for Binary Matroids

MARCEL WILD

The principal theme of the present paper is to consider isomorphism classes of binary matroids as orbits of a suitable group action. This interpretation is based on a theorem of Brylawski–Lucas. A refinement of the Burnside Lemma is used in order to enumerate these orbits. Ternary matroids are dealt with in much the same way (Section 2). Counting regular matroids is more difficult, but their number can be estimated with an arbitrarily small relative error (Section 3). Other applications of the Brylawski–Lucas Theorem include checking binary matroids for isomorphism (Section 4) and for graphicness (Section 5).

1. THE BASIC LEMMA

Let E be a finite set endowed with a closure operator $c: 2^E \to 2^E$. The pair (E, c) is called a *matroid* if, furthermore, the 'Steinitz exchange axiom' (well known from linear algebra holds):

$$(\forall A \subseteq E)(\forall p, q \in E)\ p \notin c(A) \wedge p \in c(A \cup \{q\}) \Rightarrow q \in c(A \cup \{p\}) \tag{1}$$

There are many equivalent definitions of a 'matroid'. For these and for a detailed exposition of the following concepts we refer, for example, to reference [11]. Let (E, c) be a matroid. An element p in the closure $c(\emptyset)$ of the empty set is called a *loop*. elements p and q of a matroid (E, c) which are not loops are *parallel* if $c(\{p\}) = c(\{q\})$. The matroid (E, c) is *simple* if $c(\emptyset) = \emptyset$ and $c(\{p\}) = \{p\}$ for all $p \in E$. A minimal subset $B \subseteq E$ with $c(B) = E$ is called a *base*. It turns out that all bases have the same cardinality. This common value is the *rank* of the matroid.

In Figure 1 a 6-element matroid (E, c) of rank 3 is represented by points in affine space $\mathbb{R}^2$. By definition, $p \in E$ is in $c(A)$ iff it is in the affine closure of A. This matroid is loopless but not simple, since $c(\{p_4\}) = c(\{p_5\}) = \{p_4, p_5\}$. Furthermore, for example $c(\{p_1, p_2\}) = \{p_1, p_2, p_4, p_5\}$, $c(\{p_2, p_3\}) = \{p_2, p_3\}$ and $\{p_1, p_2, p_3\}$ is a base.

Let k be a field and let $M \in k^{r \times n}$ be a matrix. We shall also write $M = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ where $\mathbf{a}_i \in k^r$ is the ith column of M. The *column matroid colmat*(M) is the matroid on $E := \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ defined by $c(\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_s}\}) := \{\mathbf{a}_j \in E \mid \mathbf{a}_j \in \langle \mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_s} \rangle\}$, where $\langle\ \rangle$ denotes the linear hull. Two matroids (E_1, c_1) and (E_2, c_2) are *isomorphic* if there is a bijection $g: E_1 \to E_2$ such that

$$g(c_1(X)) = c_2(g(X)) \qquad \text{for all } X \subseteq E_1. \tag{2}$$

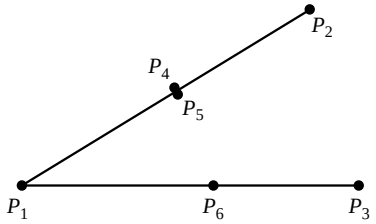

FIGURE 1.

0195-6698/96/020309 + 08 $18.00/0

A matroid (E, c) is *co-ordinatizable* over a field k if it is isomorphic to the column matroid of some matrix $M \in k^{r\times n}$. It is easy to see that r can be taken as the rank of (E, c). We shall be concerned with *binary* matroids which, by definition, are matroids that are co-ordinatizable over the 2-element field $GF(2) = \{0, 1\}$. For example, consider the 3×6 matrix M_1 over $GF(2)$ in Figure 2. It is easy to see that $colmat(M_1)$ is isomorphic to the matroid of Figure 1. Now any elementary *row* operation on a matrix does not change the dependency relations among the columns, because it amounts to multiplying each column by a certain invertible matrix. For instance, replacing row 1 in M_1 by (row 1) + (row 3) and switching row 2 with row 3 amounts to a multiplication of each column by

$$A := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and results in the matrix M_2 which represents the same matroid.

$$\underbrace{\begin{array}{cccccc} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}}_{M_1} \qquad \underbrace{\begin{array}{cccccc} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array}}_{M_2}$$

FIGURE 2.

Conversely, it is not *a priori* clear if *any* two matrices from $GF(2)^{3\times 6}$ which represent (E, c) (both labelled in the order $p_1, p_2, \ldots, p_6$) are necessarily related by a sequence of elementary row operations. Fortunately, this is true. Denoting by GL_r^2 the group of invertible $r \times r$ matrices over $GF(2)$ one has the following.

LEMMA 1 [5; 11, *Prop.* 10.1.3]. *For given matrices M_1 and M_2 in $GF(2)^{r\times n}$, let $\mathbf{a}_i$ and $\mathbf{b}_i$ be the ith column vectors of M_1 and M_2 respectively. Suppose that $\mathbf{a}_i \mapsto \mathbf{b}_i$ yields an isomorphism between the column matroids of M_1 and M_2. Then there is a matrix $A \in GL_r^2$ with $A\mathbf{a}_i = \mathbf{b}_i$ for all $1 \leqslant i \leqslant n$.*

The remainder of this paper is dedicated to several interesting consequences of this result, which apparently have gone unnoticed so far. Some of them are only outlined here and will be pursued in detail elsewhere.

2. Enumeration of Binary and Ternary Matroids

Rephrasing Lemma 1 above and using its notation, one may say that $\mathbf{a}_i \to \mathbf{b}_i$ is an isomorphism between $colmat(M_1)$ and $colmat(M_2)$ iff $rowspace(M_1) = rowspace(M_2)$. We call two r-dimensional (row) subspaces $R_1, R_2 \subseteq GF(2)^n$ *equivalent* if there is a permutation $\pi: \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $R_2 = \{(x_{\pi 1}, \ldots, x_{\pi n}) \mid (x_1, \ldots, x_n) \in R_1\}$. This is clearly an equivalence relation. In fact, it is just the usual equivalence relation between binary (n, r)-codes [cf. 4, p. 49]. By Lemma 1 the equivalence classes

also correspond bijectively to the $b(n, r)$ isomorphism classes of binary rank r matroids on n elements. It follows that

$$\frac{1}{n!}\frac{(2^n-1)(2^{n-1}-1)\cdots(2^{n-r+1}-1)}{(2^r-1)(2^{r-1}-1)\cdots(2^1-1)} \leqslant b(n, r) \leqslant \frac{(2^n-1)(2^{n-1}-1)\cdots(2^{n-r+1}-1)}{(2^r-1)(2^{r-1}-1)\cdots(2^1-1)}, \tag{3}$$

because the right-hand side equals the number of r-dimensional subspaces of $GF(2)^n$ [2, p. 78]. However, we are striving for the precise value of $b(n, r)$. For this purpose, consider the group $GL_r^2 \times S_n$, where S_n is the symmetric group on $\{1, 2, \ldots, n\}$. This group acts on the set $Z := GF(2)^{r\times n}$ of matrices $M := (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ as follows:

$$(A, \pi) * (\mathbf{a}_1, \ldots, \mathbf{a}_n) := (A\mathbf{a}_{\pi^{-1}1}, \ldots, A\mathbf{a}_{\pi^{-1}n}). \tag{4}$$

The important fact, again a trivial consequence of Lemma 1, is that the $b(n, \leqslant r)$ many isomorphism classes of binary matroids with n elements and rank $\leqslant r$ correspond bijectively to the orbits of this group action. If we put $Z_{(A,\pi)} := \{M \in Z: (A, \pi) * M = M\}$ then, by Burnside's lemma, the number of orbits equals

$$b(n, \leqslant r) = \frac{1}{|GL^2|\,|S_n|}\sum_{(A,\pi)\in GL_r^2\times S_n} |Z_{(A,\pi)}| \tag{5}$$

('average number of fixpoints'). Trivially, $b(n, r)$ is obtained as $b(n, \leqslant r) - b(n, \leqslant r-1)$. However, unfortunately equation (5) is useless for actual computation. First, it is not clear how to evaluate $|Z_{(A,\pi)}|$ for a given (A, π). Second, the number of summands is much too large: one has $|S_n| = n!$ and $|GL_r^2| = 2^{\binom{r}{2}}(2^r-1)(2^{r-1}-1)\cdots 2^1-1)$ [2, p. 94].

However, a suitable refinement of the Burnside Lemma does the job. One can show that

$$b(n, \leqslant r) = \frac{1}{|GL_r^2|\,|S_n|}\sum_{\substack{\lambda\in Part(n)\\ 1\leqslant\mu\leqslant\kappa(r)}} |C_\lambda|\,|D_\mu| \prod_{i=1}^{n} fix(\mu, i)^{a_i(\lambda)}. \tag{6}$$

Here $Part(n)$ is the family of all sequences $\lambda = (\lambda_1, \ldots, \lambda_t)$ of natural numbers satisfying $\lambda_1 + \cdots + \lambda_t = n$ and $\lambda_1 \geqslant \cdots \geqslant \lambda_t$ ('number partitions' of n). The number of j with $\lambda_j = i$ is denoted by $a_i(\lambda)$. Recall that the $\lambda \in Part(n)$ parametrize the conjugacy classes C_λ of the group S_n. Similarly, let $D_1, \ldots, D_{\kappa(r)}$ be any enumeration of the conjugacy classes of the group GL_r^2 (thus each D_μ is a similarity class of invertible matrices). By $fix(\mu, i)$ we mean the well defined number of eigenvectors (including 0) of any matrix A^i $(A \in D_\mu)$. The formula for $|C_\lambda|$ is well known, but the calculation of $|D_\mu|$ and $fix(\mu, i)$ is a bit trickier. Also, loopless and simple binary matroids respectively can be dealt with.

For instance, for $r = 12$ and $n = 25$ one has to add up $\kappa(r)\,|Part(n)| = 4053 \times 1958 \approx 8 \times 10^6$ products in formula (6). By matroid duality there are as many binary matroids on 25 elements with rank $\leqslant 12$ as there are with rank $\geqslant 13$. Hence the number of binary matroids on exactly $n = 25$ elements is $2b(25, \leqslant 12) = 58638266023262502962716$ (previously known [1] were the values for $n \leqslant 8$).

Having computed $b(n, r)$, it is interesting to evaluate the lower and upper bounds for $b(n, r)$ in (3). For instance, if $n = 5, 9, 13, 17, 21$ and $r = \lfloor n/2 \rfloor$, then (3) reads as follows:

$$\begin{array}{ccccc} 1.3 & < & 10 & < & 155 \\ 9 & < & 240 & < & 3309747 \\ 2389 & < & 29765 & < & 14877590196755 \\ 5\times 10^7 & < & 13\times 10^7 & < & 2\times 10^{22} \\ 9\times 10^{13} & < & 12\times 10^{13} & < & 4\times 10^{33} \end{array}$$

One sees that for small n both bounds are poor, but the following is probably true.

CONJECTURE. Let r be a fixed natural number. Then the lower bound in (3) asymptotically converges to $b(n, r)$ as $n \to \infty$.

Recall that by (ordinary) matroid duality one has $b(n, r) = b(n, n-r)$, i.e. 'complementarity of ranks' takes place. For *simple binary* matroids, 'complementarity of groundsets' also takes place. More precisely, denote by $sb(n, \leqslant r)$ the number of simple binary matroids of rank $\leqslant r$ on an n-element set.

THEOREM 2. *Let r, n be positive integers with $1 \leqslant n < 2^r - 1$. Then $sb(n, \leqslant r) = sb(2^r - 1 - n, \leqslant r)$.*

PROOF. Consider the $r \times (2^r - 1)$ matrix H the columns of which are the non-zero elements of $GF(2)^r$. Augment H to the $(2^r - 1) \times (2^r - 1)$ matrix M the rows of which are all non-zero linear combinations of rows from H. Put $T := \{1, 2, \ldots, 2^r - 1\}$, and for $N \subseteq T$ let $R(N)$ be the set of rows of the $(2^r - 1) \times n$ matrix the columns of which are those columns of M with indices from N ($n := |N|$). In view of Lemma 1, it suffices to prove the following. Whenever two row spaces $R(N)$, $R(N') \subseteq GF(2)^n$ are equivalent, then so are the row spaces $R(T - N)$, $R(T - N') \subseteq GF(2)^{2^r - 1 - n}$. But this is clear.† Namely, the equivalence of $R(N)$ and $R(N')$ implies the existence of a permutation $\pi: T \to T$ (which is a product of $\leqslant n$ disjoint transpositions) with $R(N') = \{(x_{\pi 1}, \ldots, x_{\pi n}) \mid (x_1, \ldots, x_n) \in R(N)\}$. Therefore, $R(T - N') = \{(y_{\pi 1}, \ldots, y_{\pi n}) \mid (y_1, \ldots, y_n) \in R(T - N)\}$, i.e. $R(T - N')$ and $R(T - N)$ are also equivalent.

A matroid is *ternary* if it is co-ordinatizable over the Galois field $GF(3)$. The analogue of Lemma 1 holds for $GF(3)$, provided that the conclusion $A\mathbf{a}_i = \mathbf{b}_i$ is replaced by $A\mathbf{a}_i = \pm\mathbf{b}_i$ (there is no $GF(q)$-analogue for $q > 3$). This leads to an enumeration of (loopless, simple) ternary matroids in much the same way. A conjecture analogous to the above is likely to hold for ternary matroids. The analogue of Theorem 2 holds for sure. Letting $st(n, \leqslant r)$ be the number of simple ternary n-element matroids of rank $\leqslant r$, one has the following.

THEOREM 3. *Let r, n be positive integers with $1 \leqslant n < \frac{1}{2}(3^r - 1)$. Then $st(n, \leqslant r) = st(\frac{1}{2}(3^r - 1) - n, \leqslant r)$.*

Besides a mere enumeration of binary or ternary matroids, an 'orderly generation' of isomorphism types (i.e. orbit representatives) is also possible; see [8] for the general group-theoretic setting. Details of most of the above, and of several numerical tables,‡ are given in [14]. See also [16].

3. ENUMERATION OF REGULAR MATROIDS

A matroid is *regular* if it is co-ordinatizable over *every* field k. For the significance of this concept see, for example, [11, ch. 13]. One can show that a simultaneously binary and ternary matroid is regular. This raises the question as to whether isomorphism classes of regular matroids can again be considered as orbits of a group action. According to Section 2 there is a group action $G2 \times Z \to Z$ the orbits of which

† I am grateful to Peter Hoffmann for opening my eyes, thereby closing the gap in [14].

‡ Independently, but with similar methods, H. Fripertinger [6] has enumerated equivalence classes of linear (n, r)-codes over $GF(q)$ ($q = 2, 3, 4, 5, 7, 8$). By a previous remark, for $q = 2, 3$ this also amounts to an enumeration of binary and ternary matroids respectively.

correspond to the $b(n, \leqslant r)$ many isomorphism classes of binary n-element matroids of rank $\geqslant r$. Similarly, there is a group action $G3 \times \bar{Z} \to \bar{Z}$ the orbits of which correspond to the $t(n, \leqslant r)$ many isomorphism classes of ternary n-element matroids of rank $\leqslant r$. Let $Z_0 \subseteq Z \times \bar{Z}$ be the set of all pairs (f, g) which yield isomorphic whence regular matroids $\{f(1), \ldots, f(n)\} \subseteq GF(2)^r$ and $\{g(1), \ldots, g(n)\} \subseteq GF(3)^r$. The group $G2 \times G3$ acts on Z_0 component-wise and the orbits correspond to the isomorphism classes of regular matroids of rank $\leqslant r$ on n elements. Unfortunately, this naive approach is most probably no longer amenable to the necessary refinement of Burnside's Lemma. Still, some other trick might do the job. For example, we could focus on the action $G3 \times \bar{Z} \to \bar{Z}$ and try to count only those orbits which represent regular matroids. Perhaps this can be interpreted as a problem of counting orbits by weight or stabilizer class (see [8]). However, probably the best one can do is to generate orbit representatives of the action $G3 \times \bar{Z} \to \bar{Z}$ *uniformly at random* (by a method of Dixon and Wilf; see, for example, [8]) and to check which ones are binary. In view of the known number of ternary matroids, this yields an estimate for the number of regular matroids the relative error of which can be chosen to be arbitrarily small. How does one check binarity? It is well known that a matroid is binary iff it cannot be contracted to a 4-element line [11, Cor. 9.1.6]. More sophisticated methods to check that a ternary matroid is binary can be found in [13]. The enumeration of regular matroids will be pursued in a forthcoming paper.

4. Testing Pairs of Binary Matroids for Isomorphism

In general, it is hard to decide whether or not two matroids are isomorphic. Of course, it matters how they are presented. Suppose that we have presentations $(E_1, \mathscr{F}_1)$ and $(E_2, \mathscr{F}_2)$, where $\mathscr{F}_i \subseteq 2^{E_i}$ is any type of set system which determines the matroid (e.g. the family of all bases, or of all hyperplanes, etc.). Then $(E_1, \mathscr{F}_1)$ is isomorphic to $(E_2, \mathscr{F}_2)$ iff there is a bijection $\pi: E_1 \to E_2$ with $\mathscr{F}_2 = \pi(\mathscr{F}_1) := \{\pi(F) \mid F \in \mathscr{F}_1\}$. In particular, $|\mathscr{F}_1| = |\mathscr{F}_2|$ is a necessary condition. Interestingly, one can do better than naively checking $|E_1|!$ many bijections.

Here is the crucial concept. For an arbitrary matrix R with entries 0, 1, define $v(R)$ as the natural number the binary representation of which is obtained by reading R line by line. Say that a matrix S is in *normal form* if $v(R) \leqslant v(S)$ for all matrices R related to S by a permutation of rows and columns. A method to transform R into normal form R^* is given in [7].

Example. Consider the matrix R shown in Figure 3(a). Without knowing the precise shape of R^*, it is clear that the row γ of maximum weight 5 comes on top, with the 1's flush left (Figure 3(b)). What does the second row of R^* look like? Row δ has three 1's below the 1's of γ and no 1's below the 0's of γ. Thus we associate the vector $x_\delta := (3, 0)$ with δ. Analogously $x_\alpha = (2, 1)$ and $x_\beta = (2, 2)$. Since x_δ is lexicographically larger than x_α and x_β, a moment's thought confirms that row δ keeps its place but with 1's flushed left (Figure 3(c)). Row δ in matrix (c) refines the partition $\{a, b, d, f, c\}$, $\{e, g\}$ induced by γ to $\{f, b, d\}$, $\{a, c\}$, $\{e, g\}$. Accordingly, rows α and β yield the auxiliary vectors $x_\alpha = (1, 1, 1)$ and $x_\beta = (1, 1, 2)$. Since x_β is lexicographically larger, row β moves up, and within each block of the partition the 1's are flushed left (Figure 3(d)). Row β refines the previous partition to $\{b\}$, $\{f, d\}$, $\{c\}$, $\{a\}$, $\{e, g\}$. The 1's of row α happen to be flushed left within these blocks already. Hence matrix (d) is the normal form R^* of R.

	a	b	c	d	e	f	g
α	1	0	0	0	1	1	0
β	0	1	1	0	1	0	1
γ	1	1	1	1	0	1	0
δ	0	1	0	1	0	1	0

(a)

	a	b	d	f	c	e	g
γ	1	1	1	1	1	0	0
δ	0	1	1	1	0	0	0
α	1	0	0	1	0	1	0
β	0	1	0	0	1	1	1

(b)

	f	b	d	a	c	e	g
γ	1	1	1	1	1	0	0
δ	1	1	1	0	0	0	0
α	1	0	0	1	0	1	0
β	0	1	0	0	1	1	1

(c)

	b	f	d	c	a	e	g
γ	1	1	1	1	1	0	0
δ	1	1	1	0	0	0	0
β	1	0	0	1	0	1	1
α	0	1	0	0	1	1	0

(d)

FIGURE 3.

The example was such that for any occurring partition of the column indices, the associated vectors x_* were *distinct.* In this case the algorithm obviously has complexity $O(m^2n)$ for $(m \times n)$-matrices R. In particular, all occurring vectors x_* are necessarily distinct when the rows of R have distinct weights. If at some stage two (or more) rows α and β yield the same lexicographical maximum $x_\alpha = x_\beta$, then things get more messy. Basically, two new branches in a 'search tree' are generated (see [7] for details).

It should be clear how all of this relates to our problem. Given matroids $(E_1, \mathscr{F}_1)$ and $(E_2, \mathscr{F}_2)$ as above, consider the $(0,1)$-matrix R_1 of size $|\mathscr{F}_1| \times |E_1|$ the rows of which are the characteristic vectors of the sets in $\mathscr{F}_1$. Analogously, R_2 is built from $(E_2, \mathscr{F}_2)$. Then $(E_1, \mathscr{F}_1)$ is isomorphic to $(E_2, \mathscr{F}_2)$ iff $R_1^* = R_2^*$. We stress that Ivanov's algorithm should be run 'column-wise' since, in general, R_i $(i = 1,2)$ has much fewer columns than rows and, moreover, the columns are unlikely to produce identical vectors x_*. This test greatly improves upon the naive approach, but it suffers from the large size of $|\mathscr{F}_i|$, which is usually of magnitude $2^{|E_i|}$. Furthermore, one has to admit that matroids are seldom given in the form $(E, \mathscr{F})$, where $\mathscr{F}$ is the family of all bases (or circuits or hyperplanes, etc.)

Very commonly, matroids are given as column matroids of matrices. In what follows we assume that our two matroids are *binary* of rank r and are presented as column matroids of $M_1, M_2 \in GF(2)^{r \times n}$. In view of Lemma 1 one can take for R_i the $2^r \times n$ matrix the rows of which constitute $rowspace(M_i)$, and run Ivanov's algorithm column-wise. The columns are now shorter than before, but one possibly has to pay the prize of more coinciding vectors x_*. We doubt that this is a serious drawback for random matroids $colmat(M_1)$ and $colmat(M_2)$. In any case, let us outline a more sophisticated approach. Consider the partition $rowspace(M_1) = \bigcup_{i=0}^{n} \mathscr{R}_{1,i}$, where $\mathscr{R}_{1,i}$ consists of all vectors of weight i. Similarly, $rowspace(M_2) = \bigcup_{i=0}^{n} \mathscr{R}_{2,i}$. If $|\mathscr{R}_{1,i}| \neq |\mathscr{R}_{2,i}|$ for some i, then the matroids are not isomorphic. Otherwise, suppose there is a canonical, *permutation-invariant* way of choosing a partial transversal $T_1 = T(rowspace(M_1))$ of $\{\mathscr{R}_{1,i}: 0 \leqslant i \leqslant n, \ \mathscr{R}_{1,i} \neq \varnothing\}$ which is a base of $rowspace(M_1)$. (Herein, 'permutation-invariant' means the following. Let π be any permutation of $\{1, \ldots, n\}$: applying π to each element of the subspace $rowspace(M_1) \subseteq GF(2)^n$ yields another subspace $V \subseteq GF(2)^n$; it is required that applying π to each element of T_1 yields precisely the vectors of $T(V)$.) Let R_1 be any $r \times n$ matrix the set of rows of

which equals T_1. Similarly, the canonical base of *rowspace*(M_2) yields the matrix R_2. Then $colmat(M_1) \simeq colmat(M_2)$ iff $R_1^* = R_2^*$. Here the normal form R_i^* can be computed very rapidly, since there are just r rows and they all have distinct weights. Of course, the crucial question is whether each *rowspace*(M) has such a canonical base. One can indeed invent a permutation-invariant notion of 'canonical', but it might not be well defined when *rowspace*(M) is highly symmetric. Without going into detail, let us mention that it is based on the following permutation-invariant concept:† the 'fingerprint' of a vector $v \in rowspace(M)$ is the tuplet $y_v = (\bar{w}\colon\ w \in rowspace(M))$, where $\bar{w}$ is the number of common positions of 1's in v and w. We trust that elaborating on the above ideas yields a decent algorithm to test binary matroids for isomorphism.

5. Testing Binary Matroids for Graphicness

A matroid is *graphic* if it is isomorphic to the polygon matroid on the edge set of some graph (see [11]). Each polygon matroid is binary. Namely, let $G = (V, E)$ be a w.l.o.g. simple graph with vertex set $V = \{v_1, \ldots, v_s\}$ and edge set $E = \{e_1, \ldots, e_n\}$. Consider the $s \times n$ matrix M the (i, j)th entry of which is 1 if v_i is incident with e_j, and 0 otherwise. Then the polygon matroid (E, c) of G is isomorphic to *colmat*(M). The weight $w(M)$ is $2n$ and each row is the sum of the other $s-1$ rows. To fix ideas, suppose that G is connected and that $n \geqslant s+2$. Then the rank of (E, c) is $r = s-1$ and there is a vertex v_i of degree $\geqslant 3$. Hence deletion of the row with label v_i results in a matrix $M' \in GF(2)^{r \times n}$ with $colmat(M') \simeq colmat(M)$ and $w(M') \leqslant 2n-3$.

Algorithm.

Input: *a matrix* $M \in GF(2)^{r \times n}$ *the column matroid* *colmat*(M) *of which is simple of rank* $r \leqslant n-2$.

Output: *if* '*no*' *then* *colmat*(M) *is not graphic*: *if* '*yes*' *then* *colmat*(M) *is graphic if* '*perhaps*' *then perhaps* *colmat*(M) *is graphic.*

Step 1: with the greedy algorithm compute a base $B := \{b'_1, \ldots, b'_r\}$ *of* *rowspace*(M) *with minimal weight* $w(B) := w(b'_1) + \cdots + w(b'_r)$. *Let* M' *be the matrix with ith row* b'_i.

Step 2: if $w(M') \geqslant 2n-2$, *then put* '*no*'.

Step 3: if $w(M') \leqslant 2n-3$ *and each column of* M' *has weight* $\leqslant 2$, *then put* '*yes*'.

Step 4: otherwise put '*perhaps*'.

The correctness of the algorithm essentially follows from the preceding remarks and from Lemma 1; *each* matrix M' with $colmat(M') \simeq colmat(M)$ has rows from *rowspace*(M). Yet a few comments are in order.

To step 1. We refer to [11, ch. 1.8] for a justification of the greedy algorithm; a trivial implementation goes like this. Let $b_1, \ldots, b_r$ be the rows of M. Produce the $2^r - 1$ non-zero elements of *rowspace*(M) iteratively as follows: $b_1,\ b_2,\ b_1+b_2,\ b_3,\ b_1+b_3,\ b_2+b_3,\ b_1+b_2+b_3,\ b_4,\ b_1+b_4, \ldots, b_1+\cdots+b_r$. A newly generated vector $b_{i_1} + \cdots + b_{i_t}$ is immediately inserted in a growing list‡ which is ordered by increasing weight. When the list is finished, take for b'_1, and b'_2 its first two vectors. As b'_i $(3 \leqslant i \leqslant r)$, pick 'greedily' the first list vector after b'_{i-1} which is not in the span of $b'_1, \ldots, b'_{i-1}$.

† R. Scharlau pointed out that my concept of an 'intersection pattern' is known as a 'fingerprint' in the theory of integral lattices.

‡ Using a *linked* list as in [9, p. 96] is actually more economical.

To step 3. A representing graph for $colmat(M)$ is easily constructed as follows. Let M'' be the matrix M' augmented by the row $b'_1 + \cdots + b'_r$. Then each column of M'' has exactly two 1's. Hence M'' defines a graph the vertices and edges of which correspond to its rows and columns respectively.

Step 4 applies if $w(M') \leqslant 2n - 3$ but some columns of M' have weight $\geqslant 3$. This can happen both for graphic and non-graphic matroids. But one easily verifies that there are at most $r - 3$ such 'bad' columns. The submatroid corresponding to the $\geqslant n - (r - 3)$ remaining columns is graphic. In fact, some test runs on random $(0, 1)$ matrices and on intentionally disturbed matrices coming from graphs respectively, have indicated that the 'perhaps' case seldom occurs.

Our algorithm has complexity $O(2^r)$ but r is just the *rank* of the given matroid $colmat(M)$. However, since a simple graphic matroid has only $n \leqslant \frac{1}{2}r^2$ elements, one still has complexity $O(2^{\sqrt{2n}}) = O(3^{\sqrt{n}})$ with respect to the cardinality n of $colmat(M)$. Thus our algorithm does not compete with the linear time method of [3]. Nevertheless, it is conceptually simpler, easier to implement and good enough for $r \leqslant 15$ or so. For large n a speed-up could be obtained by interpreting the search of a minimum weight base as an integer programming problem with $r + n$ variables. Increasing the non-deterministic character of the algorithm ('perhaps' case), one could also find codewords of small weight with a probabilistic approach, such as in [12], or by simulated annealing [10].

References

1. D. Acketa, Some results on 'small' matroids, *Coll. Math. Soc. Janos Bolyai,* **40** (Szeged 1982), 15–23.
2. M. Aigner, *Combinatorial Theory,* Springer-Verlag, Berlin, 1979.
3. R. E. Bixby and D. K. Wagner, An almost linear-time algorithm for graph realization, *Math. Op. Res.,* **13** (1988), 99–123.
4. R. Blahut, *Theory and Practice of Error Control Codes,* Addison-Wesley, Reading, Massuchusetts, 1983.
5. T. Brylawski and D. Lucas, Uniquely representable combinatorial geometries, *Colloquio Internazionale sulle Teorie Combinatorie con la Collaborazione della American Mathematical Society, 1973,* Academia nazionale dei Licei, Rome, 1976, pp. 83–104.
6. H. Fripertinger, Enumeration of isometry-classes of linear (n, k)-codes over $GF(q)$ in SYMMETRICA, *Bayreut. Math. Schr.,* **49** (1995), 215–223.
7. A. V. Ivanov, Constructive enumeration of incidence systems, *Ann. Discr. Math.,* **26** (1985), 227–246.
8. A. Kerber, *Algebraic Combinatorics via Finite Group Actions,* B.I., Mannheim/Wien/Zürich, 1991.
9. D. E. Knuth, *The Art of Computer Programming* vol. 3, Addison-Wesley, Reading, Massachusetts, 1973.
10. P. J. M. van Laarhoven, *Simulated Annealing*: *Theory and Applications, Mathematics and its applications,* D. Reidel,Dordrecht, 1987.
11. J. Oxley, *Matroid Theory,* Oxford Science Publications, Oxford, 1992.
12. J. Stern, A method for finding codewords of small weight, in: Coding theory and applications, Lecture Notes in Computer Science, vol. 388, Springer-Verlag, Berlin, 1989.
13. K. Truemper, *Matroid Decomposition,* Academic Press, Boston, 1992.
14. M. Wild, Enumeration of binary and ternary matroids and other applications of the Brylawski-Lucas Theorem, Preprint No. 1693, Technische Hochschule Darmstadt, 1994.
15. M. Wild, A theory of finite closure spaces based on implications, *Adv. Math.,* **108** (1994) 118–139.
16. M. Wild, Computations with finite closure systems and implications, in: Computing and Combinatorics, Lecture Notes in Computer Science 959, Springer Verlag, Berlin, 1995.

Received 23 January 1995 and accepted in revised form 20 April 1995

Marcel Wild
Math. Institut
Universität Zürich
Winterthurerstrasse 190
8057 Zürich
Switzerland
mwild@amath.unizh.ch